

UNITED STATES DISTRICT COURT

for the
Western District of Washington

In the Matter of the Search of

(Briefly describe the property to be searched
or identify the person by name and address)941 SW Quinalt Street, Oak Harbor, WA 98277
(SUBJECT PREMISES)

Case No. MJ19-091

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

The Subject Premises as further described in Attachment A, which is attached hereto and incorporated herein by this reference.

located in the Western District of Washington, there is now concealed (identify the person or describe the property to be seized):

See Attachment B, incorporated herein by reference.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
☒ contraband, fruits of crime, or other items illegally possessed;
☒ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
Title 18, U.S.C. § 2252 (a)(2)	Receipt or Distribution of Child Pornography
Title 18, U.S.C. § 2252(a)(4)(B)	Possession of Child Pornography

The application is based on these facts:

- ☒ See attached Affidavit continued on the attached sheet

- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

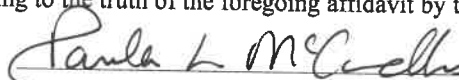
Pursuant to Fed. R. Crim. P. 4.1, this warrant is presented: ☐ by reliable electronic means; or: ☐ telephonically recorded.


Applicant's signature

SPECIAL AGENT PATRICK MIZE, HSI
Printed name and title

- ☒ The foregoing affidavit was sworn to before me and signed in my presence, or
☐ The above-named agent provided a sworn statement attesting to the truth of the foregoing affidavit by telephone.

Date: 3-6-19


Judge's signature

City and state: BELLINGHAM, WASHINGTON

PAULA L. MCCANDLIS, United States Magistrate Judge
Printed name and title

ATTACHMENT A

Description of Property to be Searched

The physical address of the SUBJECT PREMISES is 941 SW Quinalt Street, Oak Harbor, Washington 98277, and is more fully described as a property containing a two-story single-family home with a two-car garage, blue color siding with off-white trim. On the front of the house is tan numbers "941".

The search is to include all rooms, persons, and vehicles on the SUBJECT PREMISES and all garages or outbuildings, attached or detached, and any digital device(s) found therein.

ATTACHMENT B**ITEMS TO BE SEIZED**

The following records, documents, files, or materials, in whatever form, including handmade or mechanical form (such as printed, written, handwritten, or typed), photocopies or other photographic form, and electrical, electronic, and magnetic form (such as CDs, DVDs, smart cards, thumb drives, camera memory cards, electronic notebooks, or any other storage medium), that constitute evidence, instrumentalities, or fruits of violations of 18 U.S.C. § 2252(a)(2) (Receipt or Distribution of Child Pornography) and 18 U.S.C. § 2252(a)(4)(B) (Possession of Child Pornography) which may be found at the SUBJECT PREMISES:

1. Any visual depiction of minor(s) engaged in sexually explicit conduct, in any format or media;
2. Evidence of the installation and use of P2P software, and any associated logs, saved user names and passwords, shared files, and browsing history;
3. Letters, e-mail, text messages, and other correspondence identifying persons transmitting child pornography, or evidencing the transmission of child pornography, through interstate or foreign commerce, including by mail or by computer;
4. All invoices, purchase agreements, catalogs, canceled checks, money order receipts, credit card statements or other documents pertaining to the transportation or purchasing of images of minors engaged in sexually explicit conduct;
5. Any and all address books, names, lists of names, telephone numbers, and addresses of individuals engaged in the transfer, exchange, or sale of child pornography or evidencing contact with minors;
6. Any non-digital recording devices and non-digital media capable of storing images and videos.
7. Digital devices and/or their components, which include, but are not limited to:

- a. Any digital devices and storage device capable of being used to commit, further, or store evidence of the offense listed above;
 - b. Any digital devices used to facilitate the transmission, creation, display, encoding or storage of data, including word processing equipment, modems, docking stations, monitors, cameras, printers, encryption devices, and optical scanners;
 - c. Any magnetic, electronic, or optical storage device capable of storing data, such as disks, tapes, CD-ROMs, CD-Rs, CD-RWs, DVDs, printer or memory buffers, smart cards, PC cards, memory sticks, flash drives, USB/thumb drives, camera memory cards, media cards, electronic notebooks, and personal digital assistants;
 - d. Any documentation, operating logs and reference manuals regarding the operation of the digital device or software;
 - e. Any applications, utility programs, compilers, interpreters, and other software used to facilitate direct or indirect communication with the computer hardware, storage devices, or data to be searched;
 - f. Any physical keys, encryption devices, dongles and similar physical items that are necessary to gain access to the computer equipment, storage devices or data; and
 - g. Any passwords, password files, test keys, encryption codes or other information necessary to access the computer equipment, storage devices or data;
8. Evidence of who used, owned or controlled any seized digital device(s) at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, saved user names and passwords, documents, and browsing history;
 9. Evidence of malware that would allow others to control any seized digital device(s) such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malware; as well as evidence of the lack of such malware;
 10. Evidence of the attachment to the digital device(s) of other storage devices or similar containers for electronic evidence;

- 1 11. Evidence of counter-forensic programs (and associated data) that are
- 2 designed to eliminate data from a digital device;
- 3 12. Evidence of times the digital device(s) was used;
- 4 13. Any other ESI from the digital device(s) necessary to understand how the
- 5 digital device was used, the purpose of its use, who used it, and when.
- 6 14. Records and things evidencing the use of the IP addresses 76.104.222.31
- 7 (the SUBJECT IP ADDRESS) including:
- 8 a. Routers, modems, and network equipment used to connect
- 9 computers to the Internet;
- 10 b. Records of Internet Protocol (IP) addresses used;
- 11 c. Records of Internet activity, including firewall logs, caches, browser
- 12 history and cookies, "bookmarked" or "favorite" web pages, search terms that the user
- 13 entered into any Internet search engine, and records of user-typed web addresses.
- 14

15 **The seizure of digital devices and/or their components as set forth herein is**
16 **specifically authorized by this search warrant, not only to the extent that such**
17 **digital devices constitute instrumentalities of the criminal activity described above,**
18 **but also for the purpose of the conducting off-site examinations of their contents for**
19 **evidence, instrumentalities, or fruits of the aforementioned crimes.**
20
21
22
23
24
25
26
27
28

AFFIDAVIT

STATE OF WASHINGTON)

) ss

COUNTY OF WHATCOM)

I, Brian Patrick Mize, being duly sworn on oath, depose and state:

I. INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent with the U.S. Department of Homeland Security, Homeland Security Investigations (HSI), assigned to the Assistant Special Agent in Charge (ASAC) Blaine, Washington, field office. I have been employed as an HSI Special Agent and its predecessor, the U.S. Customs Service, since 2001. Prior to this assignment, I worked as a Police Officer with the St. Louis Metropolitan Police Department from 1994 to 2000. In my capacity as a Special Agent, I am responsible for conducting investigations into the numerous federal laws enforced by HSI. Since 2006, I have investigated criminal violations relating to child exploitation and child pornography, including violations pertaining to the unlawful production, importation, distribution, receipt, attempted receipt, and possession of child pornography and material involving the sexual exploitation of minors in violation of 18 U.S.C. §§ 2251, 2252(a), and 2252A(a). I am a graduate of the Federal Law Enforcement Training Center (FLETC), HSI (formally known as the U.S. Customs Service) Special Agent Training Program. My training included courses in law enforcement techniques, federal criminal statutes, conducting criminal investigations, and the execution of search warrants. I have participated in the execution of several search warrants which involved child exploitation and/or child pornography offenses and the search and seizure of computers and other digital devices. I am a member of the Internet Crimes Against Children (ICAC) Task Force in the Western District of Washington, and work with other federal, state, and local

1 law enforcement personnel in the investigation and prosecution of crimes involving the
2 sexual exploitation of children.

3 2. I am submitting this affidavit in support of an application under Rule 41 of
4 the Federal Rules of Criminal Procedure for a warrant to search the residence located at
5 941 SW Quinalt St, Oak Harbor, Washington 98277 (hereinafter the SUBJECT
6 PREMISES) and any persons located thereon, more fully described in Attachment A, for
7 the things specified in Attachment B to this Affidavit, for the reasons set forth below. I
8 also seek authority to examine digital devices or other electronic storage media. The
9 property to be searched is as follows:

10 a. 941 SW Quinalt St, Oak Harbor, Washington 98277 (the SUBJECT
11 PREMISES);

12 3. The warrant would authorize a search of the SUBJECT PREMISES, and a
13 seizure and forensic examination of digital devices found therein, for the purpose of
14 identifying electronically stored data as particularly described in Attachment B; for
15 evidence, fruits, and instrumentalities of violations of 18 U.S.C. §§ 2252(a)(2) (Receipt
16 or Distribution of Child Pornography) and 18 U.S.C. § 2252(a)(4)(B) (Possession of
17 Child Pornography).

18 4. The facts set forth in this Affidavit are based on my own personal
19 knowledge; knowledge obtained from other individuals during my participation in this
20 investigation, including other law enforcement officers; review of documents and records
21 related to this investigation; communications with others who have personal knowledge
22 of the events and circumstances described herein; and information gained through my
23 training and experience.

24 5. Because this affidavit is submitted for the limited purpose of establishing
25 probable cause in support of the application for a search warrant, it does not set forth
26 each and every fact that I or others have learned during the course of this investigation. I
27 have set forth only the facts that I believe are relevant to the determination of probable
28 cause to believe that evidence, fruits, and instrumentalities of violations of 18 U.S.C. §

2252(a)(2) (Receipt or Distribution of Child Pornography) and 18 U.S.C. § 2252(a)(4)(B) (Possession of Child Pornography), will be found at the SUBJECT PREMISES.

6. Based on the discoveries I have made, as described below, I believe that someone at the SUBJECT PREMISES has used a computer to connect to an Internet Peer-to-Peer (P2P) file sharing program, via Internet Protocol (IP) address 76.104.222.31 (hereinafter "SUBJECT IP ADDRESS"), and distributed videos depicting child pornography. I further believe that computers and other digital devices containing evidence of child pornography will be found following a search of the locations described in Attachment A.

II. DEFINITIONS

7. The following definitions apply to this Affidavit:

Internet Service Providers

a. "Internet Service Providers" (ISPs), as used herein, are commercial organizations that are in business to provide individuals and businesses access to the internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, email, remote storage, and co-location of computers and other communications equipment. ISPs can offer a range of options in providing access to the Internet including telephone-based dial up, broadband based access via digital subscriber line (DSL) or cable television, dedicated circuits, or satellite-based subscription. ISPs typically charge a fee based upon the type of connection and volume of data, called bandwidth, which the connection supports. Many ISPs assign each subscriber an account name – a user name or screen name, an "email address," an email mailbox, and a personal password selected by the subscriber. By using a computer equipped with a modem, the subscriber can establish communication with an ISP over a telephone line, through a cable system or via satellite, and can access the Internet by using his or her account name and personal password. ISPs maintain records pertaining to their subscribers (regardless of whether those subscribers are individuals or entities). These records may include account application information, subscriber and billing information,

1 account access information (often times in the form of log files), email communications,
2 information concerning content uploaded and/or stored on or via the ISP's servers.

3 Internet Protocol (IP) Addresses

4 b. "Internet Protocol address" or "IP address" refers to a unique
5 number used by a computer to access the Internet. An IP address looks like a series of
6 four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every
7 computer connected to the Internet must be assigned an IP address so that the Internet
8 traffic sent from, and directed to, that computer may be properly directed from its source
9 to its destination. Most ISPs control the range of IP addresses.

10 **III. PEER-TO-PEER (P2P) FILE SHARING**

11 8. Peer to peer (P2P) file sharing is a method of communication available to
12 internet users through the use of special software programs. P2P file sharing programs
13 allow groups of computers using the same file sharing network and protocols to transfer
14 digital files from one computer system to another while connected to a network, usually
15 on the internet. There are multiple types of P2P file sharing networks on the internet. To
16 connect to a particular P2P file sharing network, a user first obtains a P2P client software
17 program for a particular P2P file sharing network, which can be downloaded from the
18 internet. A particular P2P file sharing network may have many different P2P client
19 software programs that allow access to that particular P2P file sharing network.
20 Additionally, a particular P2P client software program may be able to access multiple
21 P2P file sharing networks. These P2P client software share common protocols for
22 network access and file sharing. The user interface, features, and configurations may
23 vary between clients and versions of the same client.

24 9. In general, P2P client software allows the user to set up file(s) on a
25 computer to be shared on a P2P file sharing network with other users running compatible
26 P2P client software. A user can also obtain files by opening the P2P client software on
27 the user's computer and conducting a search for files that are of interest and currently
28 being shared on a P2P file sharing network.

1 10. Some P2P file sharing networks are designed to allow users to download
2 files and frequently provide enhanced capabilities to reward the sharing of files by
3 providing reduced wait periods, higher user ratings, or other benefits. In some instances,
4 users are not allowed download files if they are not sharing files. Typically, settings
5 within these programs control sharing thresholds.

6 11. Typically, during a default installation of a P2P client software program,
7 settings are established which configure the host computer to share files. Depending
8 upon the P2P client software used, a user may have the ability to reconfigure some of
9 those settings during installation or after the installation has been completed.

10 12. Typically, a setting establishes the location of one or more directories or
11 folders whose contents (digital files) are made available for distribution to other P2P
12 clients. In some clients, individual files can also be shared.

13 13. Typically, a setting controls whether or not files are made available for
14 distribution to other P2P clients.

15 14. Typically, a setting controls whether or not users will be able to share
16 portions of a file while they are in the process of downloading the entire file. This feature
17 increases the efficiency of the network by putting more copies of the file segments on the
18 network for distribution.

19 15. Typically, files being shared by P2P clients are processed by the client
20 software. As part of this processing, a hashed algorithm value is computed for each file
21 and/or piece of a file being shared (dependent on the P2P file sharing network), which
22 uniquely identifies it on the network. A file (or piece of a file) processed by this hash
23 algorithm operation results in the creation of an associated hash value often referred to as
24 a digital signature. Some hash algorithms provide a certainty exceeding 99.99 percent
25 that two or more files with the same hash value are identical copies of the same file
26 regardless of their file names. By using a hash algorithm to uniquely identify files on a
27 P2P network, it improves the network efficiency. Because of this, typically, users may
28 receive a selected file from numerous sources by accepting segments of the same file

1 from multiple clients and then reassembling the complete file on the local computer.
2 This is referred to as multiple source downloads. This client program succeeds in
3 reassembling the file from different sources only if all the segments came from exact
4 copies of the same file. P2P file sharing networks use hash values to ensure exact copies
5 of the same files are used during this process.

6 16. P2P file sharing networks, including the BitTorrent network, are frequently
7 used to trade digital files of child pornography. These files include both images and
8 movie files.

9 17. The BitTorrent network is a very popular and publicly available P2P
10 sharing network. Most computers that are part of this network are referred to as “peers.”
11 The terms “peers” and “clients” can be used interchangeably when referring to the
12 BitTorrent network. A peer can simultaneously provide files to some peers while
13 downloading files from other peers.

14 18. The BitTorrent network can be accessed by computers running many
15 different client programs, some of which include the BitTorrent client program, uTorrent
16 client program, and Vuze client program. These client programs are publicly available
17 and free P2P client software programs that can be downloaded from the internet. There
18 are also BitTorrent client programs that are not free. These BitTorrent client programs
19 share common protocols for network access and file sharing. The user interfaces,
20 features, and configuration may vary between clients and versions of the same client.

21 19. During the installation of typical BitTorrent network client programs,
22 various settings are established which configure the host computer to share files.
23 Depending upon the BitTorrent client used, a user may have the ability to reconfigure
24 some of those settings during installation or after installation has been completed.
25 Typically, a setting establishes the location of one or more directories of folders whose
26 contents (files) are made available to other BitTorrent network users to download.

27 20. In order to share a file or set of files on a BitTorrent network, a “Torrent”
28 file needs to be created by the user that initially wants to share the file or set of files. A

1 "Torrent" is typically a small file that describes the file(s) that are being shared, which
2 may include information on how to locate the file(s) on the BitTorrent network. A
3 typical BitTorrent client will have the ability to create a "Torrent" file. It is important to
4 note that the "Torrent" file does not contain the actual file(s) being shared, but
5 information about the file(s) described in the "Torrent," such as the name(s) of the file(s)
6 being referenced in the "Torrent" and the "info hash" of the "Torrent." The "info hash"
7 is a SHA-1 hash value of the set of data describing the file(s) referenced in the "Torrent,"
8 which include the SHA-1 hash value of each piece, the file size, and the file name(s).
9 The "info hash" of each "Torrent" uniquely identifies the "Torrent" file on the BitTorrent
10 network. The "Torrent" file may also contain information on how to locate file(s)
11 referenced in the "Torrent" by identifying "Trackers." "Trackers" are computers on the
12 BitTorrent network that collate information about peers/clients that have recently
13 reported they are sharing the file(s) referenced in the "Torrent" file. A "Tracker" is only
14 a pointer to peers/clients on the network who may be sharing part or all of the file(s)
15 referenced in the "Torrent." It is important to note that the "Trackers" do not actually
16 have the file(s) and are used to facilitate the finding of other peers/clients that have the
17 entire file(s) or at least a portion of the file(s) available for sharing. It should also be
18 noted that the use of "Tracker(s)" on the BitTorrent network are not always necessary to
19 locate peers/clients that have file(s) being shared from a particular "Torrent" file. There
20 are many publicly available servers on the Internet that provide BitTorrent tracker
21 services.

22 21. Once a "Torrent" is created, in order to share the file(s) referenced in the
23 "Torrent" file, a user typically makes the "Torrent" available for other users, such as via
24 websites on the Internet.

25 22. In order to locate "Torrent" files of interest, a typical user will use keyword
26 searches within the BitTorrent network client itself or on websites hosting "Torrents."
27 Once a "Torrent" file is located that meets the keyword search criteria, the user will
28 download the "Torrent" file to their computer. Alternatively, a user can also search for

1 and locate “magnet links,” which is a link that enables the BitTorrent network client
2 program itself to download the “Torrent” to the computer. In either case, a “Torrent” file
3 is downloaded to the user’s computer. The BitTorrent network client will then process
4 that “Torrent” file in order to find “Trackers” or utilize other means that will help
5 facilitate finding other peers/clients on the network that have all or part of the file(s)
6 referenced in the “Torrent” file. It is again important to note that the actual file(s)
7 referenced in the “Torrent” are actually obtained directly from other peers/clients on the
8 BitTorrent network and not the “Trackers” themselves. Typically, the “Trackers” on the
9 network return information about remote peers/clients that have recently reported they
10 have the same file(s) available for sharing (based on SHA-1 “info hash” value
11 comparison), or parts of the same file(s), referenced in the “Torrent,” to include the
12 remote peers/clients Internet Protocol (IP) addresses.

13 23. For example, a person interested in obtaining child pornographic images on
14 the BitTorrent network would open the BitTorrent client application on his/her computer
15 and conduct a keyword search for files using a term such as “preteen sex.” (It should be
16 noted that this search term may not have been used in this investigation.) The results of
17 the torrent search are typically returned to the user’s computer by displaying them on the
18 torrent hosting website. The hosting website will typically display information about the
19 torrent, which can include the name of the torrent file, the name of the file(s) referenced
20 in the torrent file, the file(s) size, and the “info hash” SHA-1 value of the torrent file.
21 The user then selects a torrent of interest to download to their computer. Typically, the
22 BitTorrent client program will then process the torrent file. The user selects from the
23 results displayed the file(s) they want to download that were referenced in the torrent file.
24 Utilizing trackers and other BitTorrent network protocols (such as Distributed Hash
25 Tables, Peer Exchange, and Local Peer Discovery), peers/clients are located that have
26 recently reported they have the file(s) or parts of the file(s) referenced in the torrent file
27 available for sharing. The file(s) is then downloaded directly from the computer(s)
28 sharing the file. Typically, once the BitTorrent network client has downloaded part of the

1 file(s), it may immediately begin sharing the file with other users on the network. The
2 BitTorrent network client program succeeds in reassembling the file(s) from different
3 sources only if it receives “pieces” with the exact SHA-1 piece hash described in the
4 torrent file. During the download process, a typical BitTorrent client program displays
5 the Internet Protocol address of the peers/clients that appear to be sharing part or all of
6 the file(s) referenced in the torrent file or other methods utilized by the BitTorrent
7 network protocols. The downloaded file is then stored in the area previously designated
8 by the user and/or the client program. The downloaded file(s), including the torrent file,
9 will remain until moved or deleted.

10 24. Law Enforcement has created BitTorrent network client programs that
11 obtain information from trackers about peers/clients recently reporting that they are
12 involved in sharing digital files of known actual child pornography (based on the “info
13 hash” SHA-1 hash value), which then allows the downloading of a file from a single IP
14 address (as opposed to obtaining the file from multiple peers/clients on the network.)
15 This procedure allows for the detection and investigation of those computers involved in
16 sharing digital files of known actual child pornography on the BitTorrent network.

17 25. During the query and/or downloading process from a remote BitTorrent
18 network client, certain information may be exchanged between the investigator’s client
19 and the remote client they are querying and/or downloading a file from. Such as 1) the
20 remote client’s IP address; 2) a confirmation from the remote client that they have pieces
21 of the file(s) being requested, in whole or in part, and that the pieces of the file(s) is being
22 reported as shared from the remote client program; and 3) the remote client program and
23 version. This information may remain on the remote client’s computer system for long
24 periods of time. The investigator has the ability to log this information. A search can
25 later be conducted on a seized computer system(s) for this information, which may
26 provide further evidence that the investigator’s client communicated with the remote
27 client.
28

IV. STATEMENT OF PROBABLE CAUSE

26. In September 2018, while acting in an undercover capacity, SA Jesse Miller used a law enforcement version of BitTorrent to identify P2P users possessing and distributing image and video files depicting child pornography. SA Miller used the law enforcement version of BitTorrent to download files depicting child pornography from a P2P user at IP address 76.104.222.31 (the SUBJECT IP ADDRESS). The undercover downloads are detailed below.

27. Between September 11, 2018, at 11:11 UTC and September 13, 2018, at 5:20 UTC, SA Miller used the law enforcement version of BitTorrent to establish a single source connection with a P2P user at the IP address 76.104.222.31, the SUBJECT IP ADDRESS, who was determined to be in possession of suspected child pornography. Among the files downloaded from the SUBJECT IP ADDRESS was a video file, which I reviewed and describe below.

File: This is a five second video depicting a partially nude prepubescent female performing oral sex on an adult male. Based on her small stature compared to the adult male, youthful appearance, and lack of breast/muscular development, I estimate she is between four and seven years old.

28. On October 7, 2018, between approximately 3:40 UTC and 4:19 UTC, SA Miller used the law enforcement version of BitTorrent to establish a single source connection with a P2P user at the SUBJECT IP ADDRESS, who was determined to be in possession of suspected child pornography. Among the files downloaded from the SUBJECT IP ADDRESS was a folder containing a video file, which I reviewed and describe below.

File: This forty-nine second video depicts a nude prepubescent female lying on a bed as a nude adult male ejaculates on her genitals. The male then uses his hand to rub the ejaculate on and around her genitals. Based on her size in comparison to the male and lack of pubic/breast development, I estimate the child is under the age of twelve.

1 29. A query of a publicly available database revealed the SUBJECT IP
2 ADDRESS belonged to Comcast Communications.

3 30. In response to administrative summons seeking subscriber information,
4 Comcast Communications reported that during the dates and times of the downloads
5 described above, the SUBJECT IP ADDRESS was assigned to R. Gaffney, and the
6 service address was the SUBJECT PREMISES.

7 31. According to the Island County Assessor's Office, the SUBJECT
8 PREMISES is owned by R. and D. GAFFNEY and was purchased in 1998. Washington
9 DOL records show that R. Gaffney lists the SUBJECT PREMISES as R. Gaffney's
10 mailing address. Agents conducted surveillance at the SUBJECT PREMISES on January
11 8, 2019, and saw two cars parked on or adjacent to the SUBJECT PREMISES, both of
12 which are registered to R. and/or D. Gaffney. From my investigation, I believe their
13 adult child also resides at the SUBJECT PREMISES.

14 32. On January 8, 2018, while conducting surveillance of the SUBJECT
15 PREMISES, I used a portable electronic device to conduct a wireless survey at the front
16 of the SUBJECT PREMISES and discovered numerous Wi-Fi enabled networks. The
17 Wi-Fi networks were all locked, with one being named "Gaffney Family". I also
18 detected an "xfinitywifi" wireless internet network in the area. Based on my training and
19 experience, I know that Comcast deployed a series of wireless "hotspot" networks for
20 their customers. Comcast accomplished this by providing their wireless internet
21 customers with updated wireless routers capable of broadcasting an additional wireless
22 network. These wireless "hotspot" networks are recognized by the connecting device as
23 "xfinitywifi". Comcast customers can access "xfinitywifi" networks by logging in with
24 their unique Comcast email or username and previously created password. Of particular
25 importance is that the "xfinitywifi" networks are completely separate from the Comcast
26 customer's private home wireless network(s). While conducting a prior investigation, an
27 official confirmed that Comcast's "xfinitywifi" wireless networks are not linked or
28 connected to the Comcast subscriber's internet service. Comcast advised that a unique IP

1 Address would be assigned to the customer logging in via “xfinitywifi” and attributed to
2 that subscriber’s Comcast account.

3 33. Based on my knowledge, training, and experience, and the experience of
4 other law enforcement officers, I know that it is common for multiple individuals and
5 computers within a residence to share Internet access. I believe that someone used at
6 least one computer from the SUBJECT PREMISES to distribute child pornography via
7 an Internet based P2P file sharing program, and that evidence of that crime will be found
8 in the SUBJECT PREMISES.

9 V. PRIOR EFFORTS TO OBTAIN EVIDENCE

10 34. Any other means of obtaining the necessary evidence to prove the elements
11 of computer/Internet-related crimes, for example, a consent search, could result in an
12 unacceptable risk of the loss/destruction of the evidence sought. If agents pursued a
13 consent-based interview with any known or unknown resident(s) or occupant(s) of the
14 SUBJECT PREMISES, they could rightfully refuse to give consent and the P2P user who
15 distributed child pornography files from a computer at the SUBJECT IP ADDRESS
16 could arrange for destruction of all evidence of the crime before agents could return with
17 a search warrant. Based on my knowledge, training and experience, the only effective
18 means of collecting and preserving the required evidence in this case is through a search
19 warrant. Based on my knowledge, no prior search warrant has been obtained to search
20 the SUBJECT PREMISES.

21 VI. TECHNICAL BACKGROUND

22 35. Based on my training and experience, when an individual communicates
23 through the Internet, the individual leaves an IP address which identifies the individual
24 user by account and ISP (as described above). When an individual is using the Internet,
25 the individual’s IP address is visible to administrators of websites they visit. Further, the
26 individual’s IP address is broadcast during most Internet file and information exchanges
27 that occur.
28

1 36. Based on my training and experience, I know that most ISPs provide only
2 one IP address for each residential subscription. I also know that individuals often use
3 multiple digital devices within their home to access the Internet, including desktop and
4 laptop computers, tablets, and mobile phones. A device called a router is used to connect
5 multiple digital devices to the Internet via the public IP address assigned (to the
6 subscriber) by the ISP. A wireless router performs the functions of a router but also
7 includes the functions of a wireless access point, allowing (wireless equipped) digital
8 devices to connect to the Internet via radio waves, not cables. Based on my training and
9 experience, today many residential Internet customers use a wireless router to create a
10 computer network within their homes where users can simultaneously access the Internet
11 (with the same public IP address) with multiple digital devices.

12 37. Based on my training and experience and information provided to me by
13 computer forensic agents, I know that data can quickly and easily be transferred from one
14 digital device to another digital device. Data can be transferred from computers or other
15 digital devices to internal and/or external hard drives, tablets, mobile phones, and other
16 mobile devices via a USB cable or other wired connection. Data can also be transferred
17 between computers and digital devices by copying data to small, portable data storage
18 devices including USB (often referred to as "thumb") drives, memory cards (Compact
19 Flash, SD, microSD, etc.) and memory card readers, and optical discs (CDs/DVDs).

20 38. As outlined above, residential Internet users can simultaneously access the
21 Internet in their homes with multiple digital devices. Also explained above is how data
22 can quickly and easily be transferred from one digital device to another through the use
23 of wired connections (hard drives, tablets, mobile phones, etc.) and portable storage
24 devices (USB drives, memory cards, optical discs). Therefore, a user could access the
25 Internet using their assigned public IP address, receive, transfer or download data, and
26 then transfer that data to other digital devices which may or may not have been connected
27 to the Internet during the date and time of the specified transaction.
28

1 39. Based on my training and experience, I have learned that the computer's
2 ability to store images and videos in digital form makes the computer itself an ideal
3 repository for child pornography. The size of hard drives used in computers (and other
4 digital devices) has grown tremendously within the last several years. Hard drives with
5 the capacity of four (4) terabytes (TB) are not uncommon. These drives can store
6 thousands of images and videos at very high resolution.

7 40. Based on my training and experience, collectors and distributors of child
8 pornography also use online resources to retrieve and store child pornography, including
9 services offered by companies such as Google, Yahoo, Apple, and Dropbox, among
10 others. The online services allow a user to set up an account with a remote computing
11 service that provides email services and/or electronic storage of computer files in any
12 variety of formats. A user can set up an online storage account from any computer with
13 access to the Internet. Evidence of such online storage of child pornography is often
14 found on the user's computer. Even in cases where online storage is used, however,
15 evidence of child pornography can be found on the user's computer in most cases.

16 41. As is the case with most digital technology, communications by way of
17 computer can be saved or stored on the computer used for these purposes. Storing this
18 information can be intentional, i.e., by saving an email as a file on the computer or saving
19 the location of one's favorite websites in, for example, "bookmarked" files. Digital
20 information can also be retained unintentionally, e.g., traces of the path of an electronic
21 communication may be automatically stored in many places (e.g., temporary files or ISP
22 client software, among others). In addition to electronic communications, a computer
23 user's Internet activities generally leave traces or "footprints" and history files of the
24 browser application used. A forensic examiner often can recover evidence suggesting
25 whether a computer contains wireless software, was using Yahoo messenger, and when
26 certain files under investigation were uploaded or downloaded. Such information is often
27 maintained indefinitely until overwritten by other data.
28

1 42. Based on my training and experience, I have learned that producers of child
2 pornography can produce image and video digital files from the average digital camera,
3 mobile phone, or tablet. These files can then be transferred from the mobile device to a
4 computer or other digital device, using the various methods described above. The digital
5 files can then be stored, manipulated, transferred, or printed directly from a computer or
6 other digital device. Digital files can also be edited in ways similar to those by which a
7 photograph may be altered; they can be lightened, darkened, cropped, or otherwise
8 manipulated. As a result of this technology, it is relatively inexpensive and technically
9 easy to produce, store, and distribute child pornography. In addition, there is an added
10 benefit to the child pornographer in that this method of production is a difficult trail for
11 law enforcement to follow.

12 43. As part of my training and experience, I have become familiar with the
13 structure of the Internet, and I know that connections between computers on the Internet
14 routinely cross state and international borders, even when the computers communicating
15 with each other are in the same state. Individuals and entities use the Internet to gain
16 access to a wide variety of information; to send information to, and receive information
17 from, other individuals; to conduct commercial transactions; and to communicate via
18 email.

19 44. Based on my training and experience, I know that cellular mobile phones
20 (often referred to as "smart phones") have the capability to access the Internet and store
21 information, such as images and videos. As a result, an individual using a smart phone
22 can send, receive, and store files, including child pornography, without accessing a
23 personal computer or laptop. An individual using a smart phone can also easily connect
24 the device to a computer or other digital device, via a USB or similar cable, and transfer
25 data files from one digital device to another.

26 45. As set forth herein and in Attachment B to this Affidavit, I seek permission
27 to search for and seize evidence, fruits, and instrumentalities of the above-referenced
28 crimes that might be found at the SUBJECT PREMISES in whatever form they are

1 found. It has been my experience that individuals involved in child pornography often
2 prefer to store images of child pornography in electronic form. The ability to store
3 images of child pornography in electronic form makes digital devices, examples of which
4 are enumerated in Attachment B to this Affidavit, an ideal repository for child
5 pornography because the images can be easily sent or received over the Internet. As a
6 result, one form in which these items may be found is as electronic evidence stored on a
7 digital device.

8 46. Based upon my knowledge, experience, and training in child pornography
9 investigations, and the training and experience of other law enforcement officers with
10 whom I have had discussions, I know that there are certain characteristics common to
11 individuals who have a sexualized interest in children and depictions of children:

12 a. They may receive sexual gratification, stimulation, and satisfaction
13 from contact with children; or from fantasies they may have viewing children engaged in
14 sexual activity or in sexually suggestive poses, such as in person, in photographs, or other
15 visual media; or from literature describing such activity.

16 b. They may collect sexually explicit or suggestive materials in a
17 variety of media, including photographs, magazines, motion pictures, videotapes, books,
18 slides, and/or drawings or other visual media. Such individuals often times use these
19 materials for their own sexual arousal and gratification. Further, they may use these
20 materials to lower the inhibitions of children they are attempting to seduce, to arouse the
21 selected child partner, or to demonstrate the desired sexual acts. These individuals may
22 keep records, to include names, contact information, and/or dates of these interactions, of
23 the children they have attempted to seduce, arouse, or with whom they have engaged in
24 the desired sexual acts.

25 c. They often maintain any "hard copies" of child pornographic
26 material that is, their pictures, films, video tapes, magazines, negatives, photographs,
27 correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of
28

1 their home or some other secure location. These individuals typically retain these “hard
2 copies” of child pornographic material for many years, as they are highly valued.

3 d. Likewise, they often maintain their child pornography collections
4 that are in a digital or electronic format in a safe, secure and private environment, such as
5 a computer and surrounding area. These collections are often maintained for several
6 years and are kept close by, often at the individual’s residence or some otherwise easily
7 accessible location, to enable the owner to view the collection, which is valued highly.
8 They also may opt to store the contraband in cloud accounts. Cloud storage is a model of
9 data storage where the digital data is stored in logical pools, the physical storage can span
10 multiple servers, and often locations, and the physical environment is typically owned
11 and managed by a hosting company. Cloud storage allows the offender ready access to
12 the material from any device that has an Internet connection, worldwide, while also
13 attempting to obfuscate or limit the criminality of possession as the material is stored
14 remotely and not on the offender’s device.

15 e. They also may correspond with and/or meet others to share
16 information and materials; rarely destroy correspondence from other child pornography
17 distributors/collectors; conceal such correspondence as they do their sexually explicit
18 material; and often maintain lists of names, addresses, and telephone numbers of
19 individuals with whom they have been in contact and who share the same interests in
20 child pornography.

21 f. They generally prefer not to be without their child pornography for
22 any prolonged time period. This behavior has been documented by law enforcement
23 officers involved in the investigation of child pornography throughout the world.

24 47. In addition to offenders who collect and store child pornography, law
25 enforcement has encountered offenders who obtain child pornography from the internet,
26 view the contents and subsequently delete the contraband, often after engaging in self-
27 gratification. In light of technological advancements, increasing Internet speeds and
28 worldwide availability of child sexual exploitative material, this phenomenon offers the

1 offender a sense of decreasing risk of being identified and/or apprehended with quantities
2 of contraband. This type of consumer is commonly referred to as a 'seek and delete'
3 offender, knowing that the same or different contraband satisfying their interests remain
4 easily discoverable and accessible online for future viewing and self-gratification. I
5 know that, regardless of whether a person discards or collects child pornography he/she
6 accesses for purposes of viewing and sexual gratification, evidence of such activity is
7 likely to be found on computers and related digital devices, including storage media, used
8 by the person. This evidence may include the files themselves, logs of account access
9 events, contact lists of others engaged in trafficking of child pornography, backup files,
10 and other electronic artifacts that may be forensically recoverable.

11 48. Given the above-stated facts and based on my knowledge, training and
12 experience, along with my discussions with other law enforcement officers who
13 investigate child exploitation crimes, I believe that the user of the computer who shared
14 the child pornography described above from the SUBJECT IP ADDRESS likely has a
15 sexualized interest in children and depictions of children and that evidence of child
16 pornography is likely to be found on digital media devices, including mobile and/or
17 portable digital devices that found within the SUBJECT PREMISES.

18 49. Based on my training and experience, and that of computer forensic agents
19 that I work and collaborate with on a daily basis, I know that every type and kind of
20 information, data, record, sound or image can exist and be present as electronically stored
21 information on any of a variety of computers, computer systems, digital devices, and
22 other electronic storage media. I also know that electronic evidence can be moved easily
23 from one digital device to another. As a result, I believe that electronic evidence may be
24 stored on any digital device present at the SUBJECT PREMISES.

25 50. Based on my training and experience, and my consultation with computer
26 forensic agents who are familiar with searches of computers, I know that in some cases
27 the items set forth in Attachment B may take the form of files, documents, and other data
28 that is user-generated and found on a digital device. In other cases, these items may take

1 the form of other types of data - including in some cases data generated automatically by
2 the devices themselves.

3 51. Based on my training and experience, and my consultation with computer
4 forensic agents who are familiar with searches of computers, I believe that if digital
5 devices are found in the SUBJECT PREMISES there is probable cause to believe that the
6 items set forth in Attachment B will be stored in those digital devices for a number of
7 reasons, including but not limited to the following:

8 a. Once created, electronically stored information (ESI) can be stored
9 for years in very little space and at little or no cost. A great deal of ESI is created, and
10 stored, moreover, even without a conscious act on the part of the device operator. For
11 example, files that have been viewed via the Internet are sometimes automatically
12 downloaded into a temporary Internet directory or "cache," without the knowledge of the
13 device user. The browser often maintains a fixed amount of hard drive space devoted to
14 these files, and the files are only overwritten as they are replaced with more recently
15 viewed Internet pages or if a user takes affirmative steps to delete them. This ESI may
16 include relevant and significant evidence regarding criminal activities, but also, and just
17 as importantly, may include evidence of the identity of the device user, and when and
18 how the device was used. Most often, some affirmative action is necessary to delete ESI.
19 And even when such action has been deliberately taken, ESI can often be recovered,
20 months or even years later, using forensic tools.

21 b. Wholly apart from data created directly (or indirectly) by user-
22 generated files, digital devices - in particular, a computer's internal hard drive - contain
23 electronic evidence of how a digital device has been used, what it has been used for, and
24 who has used it. This evidence can take the form of operating system configurations,
25 artifacts from operating systems or application operations, file system data structures, and
26 virtual memory "swap" or paging files. Computer users typically do not erase or delete
27 this evidence, because special software is typically required for that task. However, it is
28 technically possible for a user to use such specialized software to delete this type of

1 information - and, the use of such special software may itself result in ESI that is relevant
2 to the criminal investigation. HSI agents in this case have consulted on computer
3 forensic matters with law enforcement employees with specialized knowledge and
4 training in computers, networks, and Internet communications. In particular, to properly
5 retrieve and analyze electronically stored (computer) data, and to ensure accuracy and
6 completeness of such data and to prevent loss of the data either from accidental or
7 programmed destruction, it is necessary to conduct a forensic examination of the
8 computers. To effect such accuracy and completeness, it may also be necessary to
9 analyze not only data storage devices, but also peripheral devices which may be
10 interdependent, the software to operate them, and related instruction manuals containing
11 directions concerning operation of the computer and software.

12 **VII. SEARCH AND/OR SEIZURE OF DIGITAL DEVICES**

13 52. In addition, based on my training and experience and that of computer
14 forensic agents that I work and collaborate with on a daily basis, I know that in most
15 cases it is impossible to successfully conduct a complete, accurate, and reliable search for
16 electronic evidence stored on a digital device during the physical search of a search site
17 for a number of reasons, including but not limited to the following:

18 a. Technical Requirements: Searching digital devices for criminal
19 evidence is a highly technical process requiring specific expertise and a properly
20 controlled environment. The vast array of digital hardware and software available
21 requires even digital experts to specialize in particular systems and applications, so it is
22 difficult to know before a search which expert is qualified to analyze the particular
23 system(s) and electronic evidence found at a search site. As a result, it is not always
24 possible to bring to the search site all of the necessary personnel, technical manuals, and
25 specialized equipment to conduct a thorough search of every possible digital
26 device/system present. In addition, electronic evidence search protocols are exacting
27 scientific procedures designed to protect the integrity of the evidence and to recover even
28 hidden, erased, compressed, password-protected, or encrypted files. Since ESI is

1 extremely vulnerable to inadvertent or intentional modification or destruction (both from
2 external sources and from destructive code embedded in the system such as a "booby
3 trap"), a controlled environment is often essential to ensure its complete and accurate
4 analysis.

5 b. Volume of Evidence: The volume of data stored on many digital
6 devices is typically so large that it is impossible to search for criminal evidence in a
7 reasonable period of time during the execution of the physical search of a search site. A
8 single megabyte of storage space is the equivalent of 500 double-spaced pages of text. A
9 single gigabyte of storage space, or 1,000 megabytes, is the equivalent of 500,000
10 double-spaced pages of text. Computer hard drives are now being sold for personal
11 computers capable of storing up to four terabytes (4,000 gigabytes of data.) Additionally,
12 this data may be stored in a variety of formats or may be encrypted (several new
13 commercially available operating systems provide for automatic encryption of data upon
14 shutdown of the computer).

15 c. Search Techniques: Searching the ESI for the items described in
16 Attachment B may require a range of data analysis techniques. In some cases, it is
17 possible for agents and analysts to conduct carefully targeted searches that can locate
18 evidence without requiring a time-consuming manual search through unrelated materials
19 that may be commingled with criminal evidence. In other cases, however, such
20 techniques may not yield the evidence described in the warrant, and law enforcement
21 personnel with appropriate expertise may need to conduct more extensive searches, such
22 as scanning areas of the disk not allocated to listed files or peruse every file briefly to
23 determine whether it falls within the scope of the warrant.

24 53. In this particular case, and in order to protect the third-party privacy of
25 innocent individuals residing in the residence, the following are search techniques that
26 will be applied:

27 i. Device use and ownership will be determined through interviews, if
28 possible, and through the identification of user account(s), associated account names, and

1 logons associated with the device. Determination of whether a password is used to lock a
2 user's profile on the device(s) will assist in knowing who had access to the device or
3 whether the password prevented access.

4 ii. Use of hash value library searches.

5 iii. Use of keyword searches, i.e., utilizing key words that are known to
6 be associated with the sharing of child pornography.

7 iv. Identification of non-default programs that are commonly known to
8 be used for the exchange and viewing of child pornography, such as, eMule, uTorrent,
9 BitTorrent, Ares, Shareaza, Vuze, Gnutella, etc.

10 v. Looking for file names indicative of child pornography, such as,
11 PTHC, PTSC, Lolita, 3yo, etc. and file names identified during the undercover download
12 of child pornography.

13 vi. Viewing of image files and video files.

14 vii. As indicated above, the search will be limited to evidence of child
15 pornography and will not include looking for personal documents and files that are
16 unrelated to the crime.

17 54. These search techniques may not all be required or used in a particular
18 order for the identification of digital devices containing items set forth in Attachment B
19 to this Affidavit. However, these search techniques will be used systematically in an
20 effort to protect the privacy of third parties. Use of these tools will allow for the quick
21 identification of items authorized to be seized pursuant to Attachment B to this Affidavit,
22 and will also assist in the early exclusion of digital devices and/or files which do not fall
23 within the scope of items authorized to be seized pursuant to Attachment B to this
24 Affidavit.

25 55. In accordance with the information in this Affidavit, law enforcement
26 personnel will execute the search of digital devices seized pursuant to this warrant as
27 follows:
28

1 a. Upon securing the search site, the search team will conduct an initial
2 review of any digital devices/systems to determine whether the ESI contained therein can
3 be searched and/or duplicated on site in a reasonable amount of time and without
4 jeopardizing the ability to accurately preserve the data.

5 b. If, based on their training and experience, and the resources
6 available to them at the search site, the search team determines it is not practical to make
7 an on-site search, or to make an on-site copy of the ESI within a reasonable amount of
8 time and without jeopardizing the ability to accurately preserve the data, then the digital
9 devices will be seized and transported to an appropriate law enforcement laboratory for
10 review and to be forensically copied ("imaged"), as appropriate.

11 c. In order to examine the ESI in a forensically sound manner, law
12 enforcement personnel with appropriate expertise will produce a complete forensic
13 image, if possible and appropriate, of any digital device that is found to contain data or
14 items that fall within the scope of Attachment B of this Affidavit. In addition,
15 appropriately trained personnel may search for and attempt to recover deleted, hidden, or
16 encrypted data to determine whether the data fall within the list of items to be seized
17 pursuant to the warrant. In order to search fully for the items identified in the warrant,
18 law enforcement personnel, which may include investigative agents, may then examine
19 all of the data contained in the forensic image/s and/or on the digital devices to view their
20 precise contents and determine whether the data fall within the list of items to be seized
21 pursuant to the warrant.

22 d. The search techniques that will be used will be only those
23 methodologies, techniques and protocols as may reasonably be expected to find, identify,
24 segregate and/or duplicate the items authorized to be seized pursuant to Attachment B to
25 this Affidavit.

26 e. If, after conducting its examination, law enforcement personnel
27 determine that any digital device is an instrumentality of the criminal offenses referenced
28 above, the government may retain that device during the pendency of the case as

1 necessary to, among other things, preserve the instrumentality evidence for trial, ensure
2 the chain of custody, and litigate the issue of forfeiture.

3 56. In order to search for ESI that falls within the list of items to be seized
4 pursuant to Attachment B to this Affidavit, law enforcement personnel will seize and
5 search the following items (heretofore and hereinafter referred to as "digital devices"),
6 subject to the procedures set forth above:

7 a. Any digital device capable of being used to commit, further, or store
8 evidence of the offense(s) listed above;

9 b. Any digital device used to facilitate the transmission, creation,
10 display, encoding, or storage of data, including word processing equipment, modems,
11 docking stations, monitors, printers, cameras, encryption devices, and optical scanners;

12 c. Any magnetic, electronic, or optical storage device capable of
13 storing data, such as disks, tapes, CD-ROMs, CD-Rs, CD-RWs, DVDs, printer or
14 memory buffers, smart cards, PC cards, memory sticks, flash drives, thumb drives,
15 camera memory cards, media cards, electronic notebooks, and personal digital assistants;

16 d. Any documentation, operating logs and reference manuals regarding
17 the operation of the digital device, or software;

18 e. Any applications, utility programs, compilers, interpreters, and other
19 software used to facilitate direct or indirect communication with the device hardware, or
20 ESI to be searched;

21 f. Any physical keys, encryption devices, dongles and similar physical
22 items that are necessary to gain access to the digital device, or ESI; and

23 g. Any passwords, password files, test keys, encryption codes or other
24 information necessary to access the digital device or ESI.

25 //

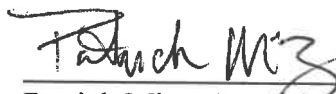
26 //

27 //

28 //

VIII. CONCLUSION

57. Based on the foregoing, I believe there is probable cause that evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 2252(a)(2) (Receipt or Distribution of Child Pornography) and 18 U.S.C. § 2252(a)(4)(B) (Possession of Child Pornography), are located at the SUBJECT PREMISES as more fully described in Attachment A to this Affidavit, as well as on and in any digital devices found therein. I therefore request that the court issue a warrant authorizing a search of the locations/person specified in Attachment A for the items more fully described in Attachment B.



Patrick Mize, Special Agent
Department of Homeland Security
Homeland Security Investigations

SUBSCRIBED and SWORN to before me this 6th day of March, 2019



PAULA L. MCCANDLIS
United States Magistrate Judge

ATTACHMENT A

Description of Property to be Searched

The physical address of the SUBJECT PREMISES is 941 SW Quinalt Street, Oak Harbor, Washington 98277, and is more fully described as a property containing a two-story single-family home with a two-car garage, blue color siding with off-white trim. On the front of the house is tan numbers "941".

The search is to include all rooms, persons, and vehicles on the SUBJECT PREMISES and all garages or outbuildings, attached or detached, and any digital device(s) found therein.

ATTACHMENT B**ITEMS TO BE SEIZED**

The following records, documents, files, or materials, in whatever form, including handmade or mechanical form (such as printed, written, handwritten, or typed), photocopies or other photographic form, and electrical, electronic, and magnetic form (such as CDs, DVDs, smart cards, thumb drives, camera memory cards, electronic notebooks, or any other storage medium), that constitute evidence, instrumentalities, or fruits of violations of 18 U.S.C. § 2252(a)(2) (Receipt or Distribution of Child Pornography) and 18 U.S.C. § 2252(a)(4)(B) (Possession of Child Pornography) which may be found at the SUBJECT PREMISES:

1. Any visual depiction of minor(s) engaged in sexually explicit conduct, in any format or media;
2. Evidence of the installation and use of P2P software, and any associated logs, saved user names and passwords, shared files, and browsing history;
3. Letters, e-mail, text messages, and other correspondence identifying persons transmitting child pornography, or evidencing the transmission of child pornography, through interstate or foreign commerce, including by mail or by computer;
4. All invoices, purchase agreements, catalogs, canceled checks, money order receipts, credit card statements or other documents pertaining to the transportation or purchasing of images of minors engaged in sexually explicit conduct;
5. Any and all address books, names, lists of names, telephone numbers, and addresses of individuals engaged in the transfer, exchange, or sale of child pornography or evidencing contact with minors;
6. Any non-digital recording devices and non-digital media capable of storing images and videos.
7. Digital devices and/or their components, which include, but are not limited to:

1 a. Any digital devices and storage device capable of being used to
2 commit, further, or store evidence of the offense listed above;

3 b. Any digital devices used to facilitate the transmission, creation,
4 display, encoding or storage of data, including word processing equipment, modems,
5 docking stations, monitors, cameras, printers, encryption devices, and optical scanners;

6 c. Any magnetic, electronic, or optical storage device capable of
7 storing data, such as disks, tapes, CD-ROMs, CD-Rs, CD-RWs, DVDs, printer or
8 memory buffers, smart cards, PC cards, memory sticks, flash drives, USB/thumb drives,
9 camera memory cards, media cards, electronic notebooks, and personal digital assistants;

10 d. Any documentation, operating logs and reference manuals regarding
11 the operation of the digital device or software;

12 e. Any applications, utility programs, compilers, interpreters, and other
13 software used to facilitate direct or indirect communication with the computer hardware,
14 storage devices, or data to be searched;

15 f. Any physical keys, encryption devices, dongles and similar physical
16 items that are necessary to gain access to the computer equipment, storage devices or
17 data; and

18 g. Any passwords, password files, test keys, encryption codes or other
19 information necessary to access the computer equipment, storage devices or data;

20 8. Evidence of who used, owned or controlled any seized digital device(s) at
21 the time the things described in this warrant were created, edited, or deleted, such as logs,
22 registry entries, saved user names and passwords, documents, and browsing history;

23 9. Evidence of malware that would allow others to control any seized digital
24 device(s) such as viruses, Trojan horses, and other forms of malicious software, as well
25 as evidence of the presence or absence of security software designed to detect malware;
26 as well as evidence of the lack of such malware;

27 10. Evidence of the attachment to the digital device(s) of other storage devices
28 or similar containers for electronic evidence;

1 11. Evidence of counter-forensic programs (and associated data) that are
2 designed to eliminate data from a digital device;

3 12. Evidence of times the digital device(s) was used;

4 13. Any other ESI from the digital device(s) necessary to understand how the
5 digital device was used, the purpose of its use, who used it, and when.

6 14. Records and things evidencing the use of the IP addresses 76.104.222.31
7 (the SUBJECT IP ADDRESS) including:

8 a. Routers, modems, and network equipment used to connect
9 computers to the Internet;

10 b. Records of Internet Protocol (IP) addresses used;

11 c. Records of Internet activity, including firewall logs, caches, browser
12 history and cookies, "bookmarked" or "favorite" web pages, search terms that the user
13 entered into any Internet search engine, and records of user-typed web addresses.

14
15 **The seizure of digital devices and/or their components as set forth herein is**
16 **specifically authorized by this search warrant, not only to the extent that such**
17 **digital devices constitute instrumentalities of the criminal activity described above,**
18 **but also for the purpose of the conducting off-site examinations of their contents for**
19 **evidence, instrumentalities, or fruits of the aforementioned crimes.**
20
21
22
23
24
25
26
27
28